Encryption Plus® Folders

Introduction

Encryption Plus® Folders delivers automatic on-the-fly encryption and protects contents of confidential files from being deleted or snooped by unauthorized persons. This enterprise version is designed for deployment across large organizations. It features full centralized administration capability, including key recovery.

Benefits

- **Protects Corporate Data with a Powerful Algorithm**
  Encryption Plus® Folders uses the well-known and documented Blowfish algorithm, a fast, 192-bit block cipher designed by Bruce Schneier.
- **Gain New Encryption Capabilities**
  In addition to folders on the hard disk, users can now encrypt folders on removable media (floppy disks, Zip® and Jaz® disks, and CD-RWs). This capability is especially valuable for two or more users who need to securely exchange or share data, as well as for backing up data and encrypting it for safe, long-term storage.
- **Easily Install & Use**
  Encryption Plus® Folders requires minimal administration and user training. It is completely transparent to the user, requiring no change in the way he/she works with the computer.
- **Maximize Your Security, Minimize Your Risk**
  Encryption Plus® Folders transparently protects data with a true "on the fly" encryption process. Other products that claim to be "on the fly" decrypt an entire file and load it into memory, creating significant security risks. Encryption Plus® Folders decrypts only the specific portion of a file that is in use.
- **Expand To Multi-User Encryption on Single Computers**
  Encryption Plus® Folders enables two or more users to share encrypted folders on a single computer. With an easy point-and-click method, a user can choose to share selected folders with any of the other Encryption Plus® Folders users listed on that computer.
- **Define Unconditionally Protected Folders**
  Administrators can define unconditionally protected folders that will always be encrypted on users' computers. For example, corporate security policy may require everyone who works at your organization to keep their confidential files in the C:\My Documents folder. If the C:\My Documents folder is unconditionally protected, it will be automatically encrypted when users install from the User Disks. Users will not have to remember to add the folder to their protected folders list, and they will not be able to unprotect the folder. This ensures that confidential documents will always be

encrypted.

- **Simplify the Login Process**
  Once integrated into the Windows® Explorer and network login, Encryption Plus® Folders no longer requires a separate login process. When the user logs into Windows® Explorer or his/her network, he/she also logs into Encryption Plus® Folders.

- **Reduce Administration Costs**
  Using RSA public/private key technology, Encryption Plus® Folders' key recovery feature ensures that corporate and local administrators can easily restore any encrypted files even if the password has been forgotten.

- **Eliminate the Danger to Unattended Computers**
  Encryption Plus® Folders automatically locks the user's keyboard and displays a password-protected Windows® screen saver.

- **Recover Forgotten Passwords Safely**
  Authenti-Check®, a special emergency password recovery feature, prevents loss of valuable data in the event the user forgets his/her password. During installation, the user has the option of writing up to three personal security questions and answers. If the user enter an incorrect password three times, Authenti-Check® is automatically activated and prompts the user to answer the security questions. If the user answers them correctly, the user will be prompted to enter a new password and will have access to the protected data.

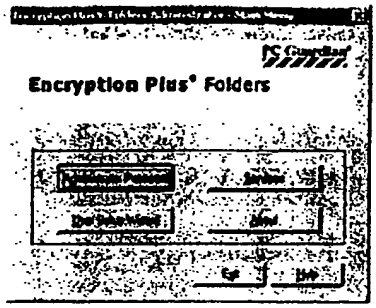
- **Secondary Authentication**
  Encryption Plus® Folders supports secondary authentication devices manufactured by third party providers, including:
  - Proximity credentials manufactured by HID.
  - eToken™ USB devices manufactured by Aladdin Knowledge Systems.

How It Works: Installation Steps & Usage

1. The administrator installs Encryption Plus® Folders Administrator on his/her workstation.
2. The administrator uses the Administrator Program to select user settings and create a User Install Disk.
3. Next, the user installs Encryption Plus® Folders on his/her workstation and selects individual folders for encryption on the hard disk.
4. Each time Windows® loads, the user is prompted for a user name and password. Alternatively, the Encryption Plus® Folders password login process can now be integrated into the Windows Explorer and network login. Thereafter, when the user logs into Windows or his/her network, he/she will also log into Encryption Plus® Folders.
5. After login, and as files located in the encrypted folder(s) are accessed, they are automatically decrypted on-the-fly with no user intervention. Likewise, the files are automatically re-encrypted on-the-fly as they are written back to the hard disk. Unauthorized users cannot access, modify or delete files in the protected folders. If necessary, the administrator has the capability to access an individual user's workstation and recover protected files.

For details on how the cryptosystems work, see the Encryption Plus Folders Technical White Paper.

Screen Shot



Click to enlarge image

System Requirements

Encryption Plus® Folders Enterprise will run on Windows 98/NT/2000/XP standard configuration.

Additional Product Resources

- Technical White Paper (PDF, 69 KB) — Details on how the Encryption Plus Folders cryptosystems work
- Support
- Administrator Manual — Version 5.0.3 (PDF, 329KB)
- User Manual — Version 5.0.3 (PDF, 256KB)

Pricing

Pricing is based on the number of end user licenses an enterprise purchases. A 50 user Starter Pack is available. Larger volume purchases receive significant discounts. For example, the per license price for 1,000 user licenses is less than the per license price for 250 licenses. Licenses are sold "in perpetuity." This means enterprises avoid annual license renewal fees.

Annual Maintenance and Support (AMS) is priced separately, is renewable, includes product upgrades, and allows subscribers on-line and telephone access to PC Guardian's comprehensive technical support resources.

Evaluation Copies

Evaluation copies of EP Folders are available to qualified enterprise buyers by completing the on-line Sales Query form.

Sales Query

Encryption grows up

Stephen Cobb. Network World. Framingham: Jul 7, 1997. Vol. 14, Iss. 27; pg. 53, 3 pgs

» Jump to full text

Subjects:	Product reviews, Software packages, Computer security, Manycompanies, Manyproducts, Perfor
Classification Codes	9190 US, 5240 Software & systems, 5140 Security management, 9172 Canada, 9120 Product spe
Locations:	US, Canada
Companies:	Entrust Technologies Ltd, McAfee Associates (Duns:60-620-5433), RSA Data Security Inc, Syma
Author(s):	Stephen Cobb
Publication title:	Network World. Framingham: Jul 7, 1997. Vol. 14, Iss. 27; pg. 53, 3 pgs
Source Type:	Periodical
ISSN/ISBN:	08877661
ProQuest document ID:	12830206
Text Word Count	2097
Article URL:	http://gateway.proquest.com/openurl?ctx_ver=z39.88-2003&res_id=xri:pqd&rft_val_fmt=ori:fmt:kev:mtx:journal&genre=article&rft_id=xri:pqd:did=00000001

More Like This »Show Options for finding similar articles

Abstract (Article Summary)

Of 5 encryption products reviewed, ⓘEntrust Technologies Inc.'s Entrust/Integrated Cryptographic Engine is the best bet for enterprise security, which is why it received Network World magazine's Blue Ribbon honors. ⓘSymantec Corp.'s Norton Your Eyes Only 4.0 has grown into a comprehensive, full feature package that comes in single-user and network versions. RSA Data Security Inc.'s SecurPC 1.1 is a solid package that now has network support while McAfee Associates Inc.'s PCCrypto 1.0.1 supports self-extracting encrypted files but encrypts archives instead of files or folders. Querisoft Inc.'s SecureFile Release Candidate 1.0 uses digital certificate technology to authenticate senders and receivers. The package's tight integration with ⓘMicrosoft products has been criticized in the cryptographic community. One negative applying to all is that they cannot talk to each other.

Full Text (2097 words)

[Headnote]
These five packages, led by Entrust/ICE, inflate the case to encrypt.

Hacked systems. Stolen laptops. Secrets sold by disgruntled employees. You've turned to firewalls, electronic locks, passwords and ID cards for protection against these threats. But your job isn't done if you're not encrypting sensitive data.

Encryption, which renders data unintelligible to anyone but the person holding the correct descrambler key, is rapidly becoming your best hope for keeping secrets secret. In fact, the five products we looked at, ranging from

offerings best-suited for single systems to packages that scale up to the enterprise, show that you no longer have as many excuses for keeping encryption out of your bag of security tricks.

Our review shows that ⓘEntrust Technologies, Inc.'s Entrust/Integrated Cryptographic Engine (ICE) is your best bet for enterprise security, which is why it received Blue Ribbon honors. The package encrypts and authenticates files and e-mail and gives you the option for more industrial-strength protection, including hardware tokens.

ⓘSymantec Corp.'s Norton Your Eyes Only (YEO) has grown into a comprehensive, mature and full-featured package that comes in single-user and network versions. RSA Data Security, Inc.'s SecurPC is a solid package that now has network support, while McAfee Associates, Inc.'s PCCrypto supports self-extracting encrypted files but encrypts archives instead of files or folders.

Finally, Querisoft, Inc.'s fledgling SecureFile uses digital certificate technology to authenticate senders and receivers. The package's tight integration with ⓘMicrosoft products, which have been criticized in the cryptographic community, has negative and positive implications.

One negative that applies to all the products is that they cannot talk to each other, which means anyone getting an encrypted file from you will need the same package to decrypt it, unless your program creates selfextracting encrypted files that can be opened by entering the correct password. This situation will not change until there is wider implementation of emerging standards such as Secure/Multi-purpose Internet Mail Extensions, IPSec, Internet Security Association & Key Management Protocol and Secure/WAN.

Entrust In public-key Infrastructure

Entrust/ICE is suitable for the enterprise because it ties desktops and laptops into the higher level Entrust and Entrust/Lite public-key infrastructures and uses pioneering digital certificate technology developed at Northern Telecom, Inc., ⓘEntrust Technologies' parent. Entrust/ICE automatically encrypts documents that have a digital signature, a unique numeric identifier that enables you to verify the identity of parties in electronic transactions.

The package also automatically encrypts the contents of designated folders using any one of an impressive range of encryp tion schemes, including ⓘNortel's proprietary Carlisle Adams and Stafford Tavares algorithm (CAST), the Data Encryption Standard, Triple-DES and RSA's RC2. You can limit access to encrypted folders to yourself or anyone on a list of recipients verified by their digital signatures. Entrust/ICE also can automatically encrypt selected files at system shutdown and decrypt them at start-up.

Entrust/ICE is well integrated with Windows 95 and NT 4.0, but requires you to license at least Entrust/Lite. When we looked at Entrust/Lite last year (NW March 11, 1996, page 57), we said it delivered a full range of high-speed encryption, authentication and verification services in a single application that is relatively easy to install and administer. Only one Entrust logon is required to access the combined encryption and file-signing features of both products.

For your eyes only

If Entrust/ICE is suited for the enterprise, ⓘSymantec's Norton YEO extends a singleuser file protection and access control utility to smaller networks.

In addition to file encryption,YEO offers a BootLock feature, which encrypts your system information to prevent intruders from accessing your hard disk. While it offers powerful protection, BootLock can render your hard drive inaccessible if something goes wrong. We strongly recommend you create an Emergency Unlock disk for insurance.

Like three of the other programs we looked at - McAfee's PCCrypto being the exception - YEO adds encryption commands to the Windows 95 or NT Explorer pop-up menu. However, YEO takes the extra step of adding an icon to the task bar for accessing the YEO Command Center, which is where you configure every aspect of data access on your PC. You can select RC4, RC5, Blowfish and Triple-DES to encrypt files, and there is an exhaustive set of password rules. The public- and private-key sizes can be set anywhere from 256 to an impressive 2,048 bits.

Any files put in a designated YEO SmartLock folder are decrypted when opened and encrypted when closed by

authorized users. The plain text copy of an encrypted file is automatically deleted, and you also have the option to wipe ordinary files from your disk with YEO's Secure Delete File command. SmartLock folders don't encrypt program files, though this can be done manually.

We had mixed feelings about the fact that SmartLock folders do not display an icon that's different from regular icons. This might add a certain amount of security-byobscurity, but authorized users might like to see at a glance which folders are encrypted, instead of having to open the Properties dialog box to check.

Other nice touches in YEO are a hotkeyactivated, passwordprotected screen saver and the ability to customize the user logon message.

YEO also offers useful features for multiple user and networked PCs. If other people use your computer, you can add them as secondary or guest users, varying the amount of access they have to your hard disk and connected network drives.

A YEO Administrator version enables you to manage encryption across an entire network. You can create users, set their rights and selectively turn on or off all options from a single console. You can define users in groups with a set of options and rights based on that group and configure password rules for everyone. When users forget their password, you can assign them a onetime password.

Furthermore, YEO Administrator lets you set a "superuser" password, which gives you the ability to override ordinary passwords. This helps avoid a data-ransoming situation in which someone tells you to pay up or you won't get the password protecting access to an important-but-encrypted file.

YEO Administrator also distributes preconfigured user modules and any updates or configuration changes, which are installed when users log on. An agent at each workstation uploads audit logs to the console so you can monitor all security-related activities.

RSA: The ⓘMicrosoft of security

Where ⓘSymantec's YEO is an extension to its traditional line of system protection utilities, RSA's SecurPC is an end-user version of the technology licensed to makers of everything from operating systems to Web browsers.

SecurPC encrypts files and folders on hard drives, diskettes and network drives. Before encrypting selected files, you are asked for your password, which can be kept in RAM to avoid repetitive re-entering. However, that comes at the risk of enabling an interloper to de-crypt files if you leave your system unattended and unlocked.

An encrypted file is given the extension .!!! with the original extension added to the file name in brackets. You use the AutoCrypt List to automatically encrypt and decrypt designated files and folders when you shut down or start up Windows. However, it would be useful if the AutoCrypt List enabled you to designate all files of a certain type for encryption.

While SecurPC won't encrypt executable or system files, it will create self-extracting encrypted files. This means the file can be sent to any Windows PC even if it isn't running SecurPC. However, Macintosh users need the version of SecurPC for their platform in order to use this feature.

To maximize performance, SecurPC uses RC4, a fast stream cipher. During setup, RC4 creates a secret key based on random mouse movements and keystrokes. The secret key is used with the user password to protect the randomly generated RC4 keys. As a safety measure, network administrators can recover encrypted files if a user's password or userpref .!!! file is lost or unavailable. An Emergency Access feature creates an emergency key that can be split into parts, each held by a different person. A minimum threshold number of key parts is then required to decrypt a user's files. Administrators also can verify who encrypted the files.

Spreading out from viruses

As RSA attempts to crack into the enduser market, McAfee is repositioning itself as a security management company. Long synonymous with antivirus software, McAfee offers its PCCrypto software as a stand-alone product

or part of its VirusScan Security Suite - formerly the Desktop Security Suite - a collection of security programs that includes a virus scanner, data backup tool, network traffic encrypter and PC firewall. McAfee recently announced Version 2.10 of PCCrypto, but we could not get it into the lab before press time. The new version, however, does not appear to be substantially different from the one we reviewed.

PCCrypto places files within encrypted archives with a .ENC extension instead of encrypting files or folders. These archives also can be converted to self-extracting files.

During installation, a program group is created on the Windows Start menu and PCCrypto is accessed from there. When running PCCrypto, you can open Windows Explorer's Select Files dialog box. You can use multiselect to add files, but you can't use wildcards or add folders. Unfortunately, there are no file types in the Files of Type dialog box. However, you can encrypt the contents of the Window's Clipboard and choose to use a 40-bit PCI algorithm, a fast stream cipher or a 160-bit Blowfish algorithm.

You can also compress plain text before encryption. The password to protect encrypted data can be up to 50 characters long and can include spaces, numbers and symbols.

Files in encrypted archives are displayed in a PCCrypto list box, allowing you to choose which ones you wish to decrypt. You're prompted for the password and warned if decrypting will overwrite an existing file. You can have details of PCCrypto operations along with your comments of up to 60 characters entered in a log file that is encrypted and password-protected. Finally, there is a facility on the wipe page to permanently erase data from your disk drive. Data that can be wiped includes disk files, file slack and free drive space, though you cannot use the wipe function on network drives.

Tightest of Windows ties

Of all the products reviewed, Atlantabased Querisoft's SecureFile has the tightest integration with Windows 95 and NT. Because the product is not yet generally available, we looked at SecureFile Release Candidate 1.0, which can be downloaded free from the company's Web site. The product primarily uses the RC4 algorithm - a 40-bit version for export and 12&bit version for domestic use - but also works with a variety of other cryptographic engines and algorithms. Like Entrust/ICE, SecureFile makes extensive use of digital signatures and certificates for authentication.

Once installed, SecureFile commands are accessed from the Windows Explorer where you can encrypt and sign files with your digital signature or encrypt files for decryption by any of the people whose certificate you have added to SecureFile.

The package can work with standard X.509 Version 3 certificates and store them in a convenient book. Currently, certificates are generated by SecureFile itself, but the package will support certificates issued by independent Certificate Authorities when they become available.

After a file has been encrypted, signed or both, SecureFile adds a .enr, .sgn or .sec extension. You can have the original file automatically deleted, but we were slightly uncomfortable that the program overwrites preexisting files without warning when an encrypted file of the same name is opened. You cannot encrypt folders using wildcards, but a handy wizard makes it relatively easy to secure files spread over different drives or folders. Only files on mapped network drives can be encrypted, as the wizard does not give you access to Windows' Network Neighborhood.

While SecureFile's tight integration with Windows is appealing in terms of ease of use, its reliance on ⓘMicrosoft's CryptoAPI could be a drawback. In order to use SecureFile, you must install Microsoft Internet Explorer 3.02 or later because SecureFile uses several updated CryptoAPI Dynamic Link Libraries that are distributed with ⓘMicrosoft's free Internet browser.

The fact that workable solutions such as the five we examined are available is reducing your ability to argue against using encryption.

Using encryption as your last line of defense against malicious intruders or misguided insiders makes a lot of sense in today's increasingly interconnected world, particularly when you factor in the fallibility of other security

technologies. Not to mention that it could save a lot more than your data.

[Author Affiliation]
Cobb is a certified IS security professional and head of Cobb Associates, an IT and security consultancy in Titusville, Fla. He can be reached at cobb@digital.net.

---

^ Back to Top « Back to Results < Previous Article 9 of 9 Publisher Information
Print Email Mark Article Abstract, Full Text, Page Image - PDF